LUSU Data Protection Policy

Approved by: LUSU Trustee Board On: 21 June 2016
Implementation Date: 23 June 2016
Review Date: 23 June 2017
Policy Owner: LUSU Trustee Board (Chief Executive Officer)

1. Introduction & Data Protection Principles

1.1 The Data Protection Act 1998 requires organisations, including Lancaster University Students' Union, to ensure that information it holds on individuals is stored appropriately. In line with this, Lancaster University Students' Union is registered with the Information Commissioner as a Data Controller. The purpose of the Act is to protect the rights and privacy of individuals, and to ensure, wherever possible, that data about them is not processed without their knowledge and is processed with their consent.

1.2 Lancaster University Students' Union is fully committed to compliance with the requirements of the Data Protection Act 1998 which came into force on 1st March 2000 and recognises in full the rights and obligations established by the Act in relation to the management and processing of personal data. The EU GDPR will come into force in 2018. This policy will need to be replaced to comply with its requirements and LUSU will need to review whether its processing meets GDPR requirements.

1.3 This policy is intended to serve as general guidance for staff and students in implementing the letter and spirit of the provisions and principles of the Act. The Union will therefore follow procedures which aim to ensure that all members, elected officers, employees, contractors, agents, consultants, or other partners of the Union who have access to any personal data held by or on behalf of the Union, are fully aware of and abide by their duties under the Data Protection Act 1998.

1.4 In the first instance an appointed Data Protection Officer will have responsibility for the Data Protection Policy. The Trustee Board has the authority to make revisions to the policy. The Union's Data Protection Officer will be responsible for bringing forward any revisions to the Board.

2. Statement of Policy

2.1 In order to operate efficiently, the Lancaster University Students' Union has to collect and use information about people with whom it works. These may include members of the Union, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

2.2 This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

2.3 The Union regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between itself and those with whom it carries out business.

2.4 The Union will ensure that it treats personal information lawfully and correctly. To this end the Union fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act 1998.

3. The 8 principles of Data Protection

3.1 The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable. The Principles require that personal information shall:

3.1.1 Be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

3.1.2 Be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purposes;

3.1.3 Be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

3.1.4 Be accurate and where necessary, kept up to date;

3.1.5 Not be kept for longer than is necessary for that purposes;

3.1.6 Be processed in accordance with the rights of data subjects under the Act;

3.1.7 Be kept secure i.e. protected by an appropriate degree of security;

3.1.8 Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

3.2 The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and “sensitive” personal data.

4. Definitions

4.1 **Personal Data:** Data which relate to a living individual who can be identified from the data, or from the data and other information about the individual which is in the possession of or is likely to come into the possession of the data controller. Personal data includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.2 **Personal Sensitive Data:** Personal data relating to racial or ethnic origins, political opinions, religious beliefs, union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences and criminal proceedings.

4.3 **Processing:** The obtaining, recording, holding, organizing, combining, altering, retrieving, consulting, disclosing, disseminating, deleting, destroying or otherwise using the data.

4.4 **Data Controller:** A person or organisation who determines the purposes for which and the manner in which any personal data, are, or are to be, processed.

4.5 **Data Processor:** Any person (other than an employee of the data controller) who processes the data on behalf of the data controller, (described in the 1984 Act as a computer bureau).

4.6 **Data Subject**: A living individual who is the subject of the personal data.

4.7 **Third Party:** Any person other than a data subject or the data controller or any data processor or other person authorised to process data for the data controller or processor.

5. Implementation, Support & Guidance

5.1 All career staff, student staff, officers and volunteers within the union must be aware of the need to handle personal data in line with the Data Protection Act 1998. On commencement of employment or prior to gaining access to systems as a volunteer an individual will complete the training specified under Responsibilities & training.

5.1.1 This will be recorded within the Union's student or the online training record.

5.1.2 The Data Protection Officer for Lancaster University Students' Union will be responsible for:

5.1.3 Implementing and monitoring the Data Protection Policy

5.1.4 Cascading the provision of training for staff, volunteers and student groups

5.1.5 Developing best practice guidelines

5.1.6 Carrying out compliance checks to ensure adherence with the Data Protection Act

5.2 Designated officers have also been identified across all departments and will be responsible for making sure the policy is implemented under the guidance of the designated Data Protection Officer.

5.3 The Data Protection Officer should be informed of all data subject requests received by staff or student groups within the union.

5.4 Advice on specific issues concerning the handling of personal data may also be contained within the relevant policy and are outlined in Appendix A.

6. Consent

6.1 In order for personal data to be processed fairly and lawfully, it is usually appropriate that the data subject has given his/her consent. This is particularly important if the personal data is classed as 'sensitive', as defined under the Act. It is not always possible or appropriate to obtain consent. Processing of personal data can take place when any condition from Schedule 2 of the DPA is met. For sensitive personal data, one condition from Schedule 2 must be met.

6.2 Consent for general activity and data linked to or from the core union database will be gained as part of the University registration process on or before UK implementation of the EU General Data Protection Regulation. Any additional information gathered will link to this policy and have a reference in appendix A to explain the parameters around its use.

7. Transfer of Personal Data

7.1 Lancaster University Students Union may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

7.1.1 The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

7.1.2 The data subject has given his consent.

7.1.3 The transfer is necessary for one of the reasons set out in the Data Protection Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

7.1.4 The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

7.1.5 The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

7.2 Subject to the requirements of 7.1 above, personal data held may also be processed by staff operating outside the EEA who work for us or one of our suppliers. That staff may be engaged in, amongst other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

8. Responsibilities & Training

Area	Data	Responsible Manager	Accessed By	Minimum Training Provided
General Info	Name, Address & Contact Details, Membership of Groups, Next of Kin, Communications	Head of Comms & IT	LUSU staff, Full Time Officers, Group Admins	University Data Protection Training (Staff or student version)
Advice Service	Information relating to case work	Education and Support Manager	LUSU Staff	University Data Protection Training. Specific staff inductions.
Colleges	Event Attendance, college membership	Student Engagement Manager (Colleges)	LUSU staff, Full Time Officers, JCR Admins	University Data Protection Training (Staff or student version)
Democracy	Electoral roll, Voting stats, demographic breakdowns	Education and Support Manager	LUSU staff, Full Time Officers	University Data Protection Training
Finance	Information relating to salaries, bank accounts,	Financial Controller	Finance team	University Data Protection training
Accommodation	Addresses and phone numbers, emails, home address,	LUSU Living Manager	LUSU staff, contractors to facilitate property services	University Data Protection training
Human Resources Career Staff	Personal information relating to salary, contract details,	Departmental Administrator	Management team	University Data Protection training

Human Resources Student Staff	Personal information relating to salary, contract details,	Head of Comms & IT	Student Line Managers & Supervisors	University Data Protection training
Marketing	Marketing preferences, usage of website and services	Commercial Marketing and Support Manager	LUSU staff, Full Time Officers	University Data Protection training
Overseas Team	Information relating to students travelling overseas including medical / health details, bank accounts, next of kin	International Programme Manager	LUSU staff	University Data Protection training
Sugarhouse	Attendance, CCTV, spending information	Sugarhouse Venue Manager	LUSU staff	University Data Protection training
Student Groups	Information on all students in online membership system	Student Engagement Managers	LUSU staff, Group admins	University Data Protection training
Schools	Volunteer information, contact information, placement details	Schools Outreach Manager	LUSU staff	University Data Protection training
Student Media	Membership information, attendance at events	Head of Communications and IT	LUSU staff, Full Time Officers	University Data Protection training

9. Subject Access

9.1 The Act gives data subjects the right to access to their personal data held by Lancaster University Students' Union. A request must be made in writing (and this includes e-mail requests), and a £10 administrative fee paid.

9.2 This entitles the individual to be told by Lancaster University Students' Union whether they are processing that individual's personal data, the purposes for which they are being processed, to whom they are or may be disclosed and to receive in an intelligible manner, a copy of their personal data.

9.3 Lancaster University Students' Union will, in some circumstances and at the discretion of the CEO and/or President, waive payment of the fee.

9.4 Lancaster University Students' Union must ensure that it has proof of the identity of the requestor to prevent an unlawful disclosure.

9.5 A data subject can request access to their personal data through another party such as a lawyer or an advocate. A signed letter or form of authority from the data subject must be provided before any data is disclosed.

9.6 Lancaster University Students' Union is required by the Act to respond within 40 calendar days of receipt of the request and the fee, but every effort should be made to respond as quickly as possible. The 40 days applies to all requests for personal data, whether routine or complex.

9.7 If the request arises as part of another matter for instance a complaint, grievance or disciplinary matter, the requirements of the DPA must not be overlooked, particularly the 40 day deadline. In these circumstances, staff must seek advice from the Data Protection Officer.

9.8 The requested data should normally be provided in permanent form on paper.

9.9 If an individual feels they are being denied access to personal information they are entitled to, or feel that their information has not been handled according to the eight principles, they can contact the Information Commissioners Office: www.informationcommissioner.gov.uk.

10. Sharing of Personal Information

10.1 Lancaster University Students Union may share personal data held with any member of the Union's group, which means any limited company whose share capital is held entirely by Lancaster University Students Union.

11. Inaccurate Information

11.1 If the data subject believes that their personal data is inaccurate, out-of-date, held unnecessarily or is offensive, they have the right to have the information rectified, blocked, erased or destroyed. The data subject also has the right to insist that Lancaster University Students' Union ceases to process their personal data if such processing is causing or is likely to cause unwarranted substantial damage or substantial stress to them or to another. The data subject may also have a right to compensation if it can be proven that damage or distress has been caused.

11.2 Lancaster University Students' Union will ensure that personal data held is accurate and kept up to date. It will take all reasonable steps to destroy or amend inaccurate or out of date data.

12. Breach Management

12.1 The purpose of breach management is to ensure the breach has stopped, understand the impact of the breach, report to relevant parties the occurrence and to investigate and make changes so a repetition of the breach does not occur.

12.2 The following steps will be undertaken:

12.2.1 Breach secured to ensure no more data leaked

12.2.2 Investigation led by the Data Protection Officer. The University will be informed and consideration will be taken as to whether the breach is reportable to the ICO

12.2.3 Anyone affected by breach contacted and any action they can/should take explained

12.2.4 Recommendations made to the management team around changes to processes to ensure no repetition of a similar breach occurs

13. Handling Procedures

13.1 Lancaster University Students' Union will, through appropriate management and the use of strict criteria and controls;

13.2 Observe fully conditions regarding the fair collection and use of personal information;

13.3 Meet its legal obligations to specify the purpose for which information is used;

13.4 Collect and process appropriate information and only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;

13.5 Ensure the quality of information used;

13.6 Apply strict checks to determine the length of time information is held;

13.7 Take appropriate technical and organisational security measures to safeguard personal information;

13.8 Ensure that personal information is not transferred abroad without suitable safeguards;

13.9 Ensure that the rights of people about whom the information is held can be fully exercised under the Act. These include:

13.10 The right to be informed that processing is being undertaken;

13.11 The right of access to one's personal information within the statutory 40 days;

13.12 The right to prevent processing in certain circumstances;

13.13 The right to correct, rectify, block or erase information regarded as wrong information.

13.14 Entire Organisation

13.15 In order that our obligations are met the Union will ensure:

13.16 There is someone with specific responsibility for data protection in the organisation;

13.17 Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;

13.18 Everyone managing and handling personal information is appropriately trained to do so;

13.19 Everyone managing and handling personal information is appropriately supervised;

13.20 Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;

13.21 Queries about handling personal information are dealt with promptly and courteously;

13.22 Methods of handling personal information are regularly assessed and evaluated;

13.23 Performance with handling personal information is regularly assessed and evaluated;

13.24 Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

14. Staff & Officers of the Union

14.1 All elected officers are to be made fully aware of this policy and of their duties and responsibilities under the Act.

14.2 All managers and staff within the Union will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

14.3 Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;

14.4 Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;

14.5 Individual passwords should be such that they are not easily compromised.

14.6 All breaches of data protection will be reported to the Data Protection Officer

14.7 Computers/Devices are locked when not attended

15. 3rd Parties

15.1 All contractors, consultants, partners or other agents of the Union must:

15.1.1 Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Union, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act.

15.1.2 Agree that any breach of any provision of the Act will be deemed as being a breach of any contract between the Union and that individual, company, partner or firm;

15.1.3 Allow data protection audits by the Union of data held on its behalf (if requested);

15.1.4 Indemnify the Union against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

16. Appendix A: Data Stored by the Union & Subsidiary Companies

Data	Reason for retention period	Retention Period	Area Responsible	Action following retention period
Student Data and Membership of Groups and Officerships	Data kept as part of historic record for reference back at any time. This data is used by alumni and also for references around jobs.	Indefinite	I.T.	
Health Forms & Next of Kin	Kept during trip related activity or activities and for a period after in case of problems that don't become immediately apparent	End of activity(ies) + 6 months	Event/Activity Organiser	Secure destruction of forms
School and community placements	Kept to refer back for placement in future years	Indefinitely	Schools / Community	
Tickets purchase and event attendance	Used to give information about related events and activity and for potential refunds or complaints. Kept for 4 years to allow for average attendance at University	4 years after event	Data Protection Officer	Event destroyed within system
Passport copies	Used during outbound activity. Kept for 6 months after in case of incident	Within 6 months from trip completion	Trip Organiser	Securely destroyed
Driver Details	Driving license copies for insurance purposes	Driving licence kept for duration student/staff is driving for LUSU. Insurance info kept for one year after	Activities Team, Schools Team,	Securely destroyed

		expiry of policy		
Case Notes	Legislation around advice and casework	6 years after case opened	Ed & Support	Automatic deletion by Advice Pro
Housing Contracts and Tenancy information	Kept in line with legislation as record of residence and for financial records	6 years	Housing	Deletion from system and paper record shredded
Bank records	Kept for reimbursement or payment refunds	6 months after end of related activity	Finance	Secure deletion / shredding
Client & Local Business Information	Kept whilst business trading and working with organisation	3 years after disengagement	Marketing	Deleted from system
CCTV	Crime detection and At least 90 days then automatically deleted.	Minimum 90 days. Incidents 5 years.	Sugarhouse	Data over-written as space requires. Specific incidents kept for 5 years.
Still images of guest ID	Verification of guests within venue. Incidents reported within 3 days.	72 hours	Sugarhouse	Deleted from system

17. Appendix B: Data Processors Used by the union

Processor Name	Data Processed	Service Liaison	Approved By	Rationale
Campaign Monitor	Email & Demographic Information	Comms Manager	Information Compliance Manager	Student data passed with permission from student. Specific models of security provided by company to ensure meets EU legislation. Same provider as University
Find my Shift	Personnel and shift information	Head of IT & Comms	n/a	UK Based company with adequate protection of data. Minimal information stored and not passed from University records
Freshdesk	Email and information specific to interactions around service delivery	Comms Manager	n/a	US Based company providing adequate protection of data. Minimal information stored and not passed from University records. Information only passed from action by student.
Studentpad	Student accommodation and contact information	LUSU Living Manager	n/a	UK Based company with adequate protection of data. Minimal information stored. Same provider as University
Union Cloud	Student information, group membership, event attendance, demographic data	Head of IT & Comms	Information Compliance Manager	EU Based storage with adequate protection of data. Agreed with University Data Protection Officer
Sage/Datel	Bank Accounts	Financial Controller	n/a	Stored on-site with adequate security. Minimal information stored with express consent.
Zoho	Client contact details & Contracts	Marketing Manager	n/a	US based with adequate security storing client details of local businesses. No data passed from

				University.
Atlantic Data	DBS Checks	Schools Outreach Manager	University managed system	UK Based and UK Hosted and ISO2701 certified and used by the University and contracted through them.
Advice Pro	Casework Information	Education & Support Manager	n/a	UK Based company and storage. Adequate protection. Relied upon sector wide.
Wufoo	Various forms submitted by students	Student Engagement Manager (colleges)	n/a	EU Based company not used to store personal information.
Lancaster University	Various data	Head of IT & Comms		Adequate security based in UK and follows same rules or more stringent ones. Main source of personal data. Keep student information within University systems whenever possible.

18. Appendix C: Education & Support Confidentiality Policy

LUSU EDUCATION & SUPPORT CONFIDENTIALITY POLICY

"A confidential service – nothing you tell us will be shared with anyone outside the service without your permission. With your permission we will contact relevant organisations and individuals in order to assist you. We will not contact anyone you expressly ask us not to. Confidentially will only ever be set aside if it is perceived you pose a serious immediate danger to yourself or to others "

We're committed to providing a confidential advice service and believe that principles of confidentiality must be integrated across all aspects of services and management. Users deserve the right to confidentiality to protect their interests. Our policy is displayed in the waiting area, interview rooms as well as here on our website.

LUSU Education & Support recognises that clients need to feel secure in using the service in a confidential manner.

1. No information regarding a client shall be given directly or indirectly to any third party external to the advice team without the clients expressed permission.
2. Clients should be able to access its services in confidence and that no other person ever know that they have used our services. All staff should ensure that no discussions identifying individual clients of the service take place outside of the service.
3. We will ensure that clients are offered confidential interview space.

CASE MANAGEMENT SYSTEM

To manage cases and represent students effectively, we do keep information relating to clients on a secure case management system. This includes case notes, copies of correspondence, calculation sheets and any other sources of information. The system can only be accessed by staff. Case files remain the property of the service although clients can be given access and photocopies of their own case records on request. Records will be kept for 6 years after which time they will be confidentially disposed of.

We're also committed to effective statistical recording to enable LUSU Education and Support to monitor service take-up and identify arising policy issues. Any statistical records given to third parties, such as to support funding applications, monitoring reports for the LUSU management or executive shall be produced in anonymous form, so individuals cannot be recognised unless their express consent has been given.

CONSENT TO GIVE INFORMATION

It is the responsibility of advisers to ensure that where action is agreed to be taken on behalf of a client, that client must firstly have been asked if there is anyone they do not wish LUSU to contact. The client's response will be recorded in their case file.

The advisers are responsible for checking with clients that it is acceptable to call or write to them at home or work in relation to their case. All staff must ensure they make no reference to the service to third parties when making telephone contact with clients.

All details of consent or requests not to disclose information will be recorded in the case file.

BREACH OF CONFIDENTIALITY

We recognise that occasions may arise where individual advisers feel they need to breach confidentiality. However, any breach of confidentiality will be treated very seriously. When an adviser feels confidentiality should be breached the following steps will be taken:

- The adviser should where possible discuss the potential breach with the client.
- The adviser should raise the matter immediately with their line manager who will discuss with them the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved by breaching confidentiality. The manager will make written notes of the discussion, which will be added to the clients file.
- It is the responsibility of the line manager to discuss the available options for each case with the adviser.
- The line manager is responsible for making the decision on whether confidentiality should be breached. If it is decided that confidentiality is to be breached then the following steps are to be taken:

If the breach of confidentiality is authorised, a full written report should be made and a copy included in the case file.

Under no circumstances should any breach of confidentiality be discussed with anyone who would be in a position to investigate a complaint against LUSU Education & Support. This is to ensure that any future complaints or investigations arising from the breach in confidentiality can be carried out in an independent manner.

If the decision is urgent and the line manager is absent, all the adviser will liaise with the Chief Executive or their deputy who will nominate another member of the senior management team to help resolve the matter.

LEGISLATIVE FRAMEWORK

We will monitor this policy to ensure it meets statutory and legal requirements including the Data Protection Act, Children's Act, Rehabilitation of Offenders Act, Social Security Administration (Fraud) Act, Prevention of Terrorism Act and Human Rights Act.

CONFLICT OF INTEREST

Confidentiality will need to be breached when LUSU Education & Support identifies a conflict of interest, which necessitates informing one party that LUSU Education & Support can no longer act on their behalf. By its very nature this will draw attention to the fact that LUSU Education & Support is acting for the other party. This is the only information, which should be disclosed and therefore would not be a breach of this policy.

ENSURING THE EFFECTIVENESS OF THE POLICY

Existing and new staff will be introduced to the Confidentiality Policy via induction and training. The policy will be reviewed annually and all SU Executive members will receive a copy of it. Copies will be available to students on request.

CONFLICTS OF INTEREST

- There is duty is upon the adviser to identify any conflicts of interest in a timely manner to limit any potential impacts on their service to the student
- If an adviser feels that they are unable to offer advice or support to a particular student or group of students due to suspected conflict of interest, they should refer the case to another Adviser or to an alternative service provider. [There is no need to disclose the nature of a conflict of interest to other advisers merely that one exists].
- If a conflict of interest arises between students or groups of students, we cannot guarantee to provide impartial advice and support for both parties. The first party to approach the service will, if possible, receive that help.
- It may be suggested that LUSU acts as a mediator between the parties, but only if both parties are in agreement.
- In circumstances where a complaint or dispute is against another LUSU service or member of staff
- Will ensure that the student understands that there is a potential conflict of interest.
- If both the adviser and the student are happy to continue in this knowledge then the case can proceed.
- If at any point the student or adviser feels unable to continue, the student will be referred to an alternative service provider or made aware of the complaints procedure.

- A 3rd party should handle complaints directly against other members of the advice team.